COMPUTER SYSTEMS, IN PARTICULAR VIRTUAL PRIVATE NETWORKS

Abstract

A first node (client) (1) is in communication with one of a plurality of second nodes (5, 6, 7) connected to a local area network (LAN) (4) via a virtual private network including a link (3), such as the Internet, and a selected one of a plurality of third nodes (gateway servers) (21, 22, 23). Communication between the first node (1) and the third nodes (21, 22, 23) is encrypted, whereas communication between the third nodes and the second nodes (5, 6, 7) is unencrypted. Communication from the first node (1) to one of the second nodes (5, 6, 7) is initially set up via a selected one of the third nodes after suitable authentication. If that third node should subsequently fail, an alternative third node can be used. To detect the failure of a third node, the first node (1) sends a "heartbeat" packet (failure detection signal) to it. An operational third node responds with an answer, indicating that all is well. If no answer is received within a predetermined time interval, the first node sends another "heartbeat" packet. If there is still no answer, another third node is selected for use. This other third node can be one that was previously authenticated, or alternatively one that must be authenticated at this time. In order to reduce workload heartbeat messages may only be sent at selected times. (Fig.2)